



manuel de supervision des ordinateurs de bureau

station de travail hp xw4000

station de travail hp xw6000

Référence : 301201-051

Octobre 2002

Le présent manuel fournit des définitions et des instructions pour l'utilisation des fonctions de sécurité et de Supervision intelligente préinstallées sur certains modèles.

© 2002 Hewlett-Packard Company

Compaq, le logo Compaq, ROMPaq, and iPAQ sont des marques de Compaq Information Technologies Group, L.P aux États-Unis et dans d'autres pays.

Microsoft, MS-DOS, Windows et Windows NT sont des marques déposées de la société Microsoft aux États-Unis et dans d'autres pays.

Intel, Pentium, Intel Inside et Celeron sont des marques de Intel Corporation aux États-Unis et/ou dans d'autres pays.

Tous les autres noms de produits mentionnés dans le présent document sont des marques appartenant à leurs détenteurs respectifs.

Hewlett-Packard Company ne pourra être tenue responsable des omissions ou des erreurs de nature rédactionnelle ou technique pouvant subsister dans ce document, ni de dommages directs ou indirects causés par la fourniture, le fonctionnement ou l'utilisation de ce matériel. Les informations de ce documents sont fournies "en l'état", sans garantie d'aucune sorte, y compris une quelconque garantie implicite de capacité marchande et d'aptitude à remplir un but particulier ; elles peuvent également faire l'objet de modifications sans préavis. Les garanties applicables aux produits HP sont énoncées dans les certificats de garantie limitée accompagnant ces produits. Aucun élément de ce document ne peut être considéré comme une garantie supplémentaire.

Ce document contient des informations protégées par des droits d'auteur. Aucune partie de ce document ne peut être photocopiée, reproduite ou traduite dans une autre langue sans l'accord écrit au préalable de Hewlett-Packard Company.



AVERTISSEMENT : le non-respect de ces instructions expose l'utilisateur à des risques potentiellement très graves.



ATTENTION : le non-respect de ces instructions présente des risques pour le matériel et les informations qu'il contient.

manuel de supervision des ordinateurs de bureau
station de travail hp xw4000
station de travail hp xw6000
Première édition (octobre 2002)
Référence : 301201-051

Table des matières

Manuel de supervision des ordinateurs de bureau

Configuration et mise en œuvre initiales.	2
Installation de système à distance	3
Mise à jour et gestion des logiciels	3
Altiris eXpress	4
Altiris eXpress PC Transplant Pro	5
Altiris eXpress HP/Compaq Client Manager	6
System Software Manager	6
Product Change Notification	7
ActiveUpdate	7
Réécriture de la ROM	8
Réécriture de la ROM à distance	8
Bloc d’amorçage ROM FailSafe.	9
Réplication de la configuration.	11
Bouton d’alimentation double état	11
Gestion de l’alimentation	12
Site Web	13
Composantes et partenaires	13
Desktop Management Interface (DMI).	14
Wired for Management.	14
Suivi d’inventaire et sécurité.	15
Sécurité par mot de passe	18
Suppression d’un mot de passe de mise sous tension ou de configuration.	22
Mode Serveur réseau	24
DriveLock	24
Détecteur Smart Cover	27
Verrou Smart Cover	28
Sécurité MBR (Master Boot Record)	31
Dispositif antivol.	34
Identification des empreintes digitales	34

Notification des pannes et récupération	34
Système de protection d'unité DPS	35
Surveillance de l'intégrité Ultra ATA	35
Alimentation avec protection contre les surtensions	35
Détecteur thermique	35

Index

Manuel de supervision des ordinateurs de bureau

HP fut le pionnier de la supervision des ordinateurs de bureau en produisant dès 1995 les tout premiers ordinateurs personnels entièrement supervisés. Depuis, HP est devenu un leader du marché en matière de développement de normes et d'infrastructures nécessaires pour déployer, configurer et superviser efficacement des ordinateurs de bureau, des stations de travail et des ordinateurs portables. La Supervision intelligente de HP offre des solutions normalisées pour la supervision et le contrôle de ces systèmes dans un environnement réseau. HP travaille en étroite collaboration avec les principaux éditeurs de logiciels de supervision, de manière à assurer la compatibilité entre la Supervision intelligente et leurs produits. La Supervision intelligente est un élément important de notre engagement à vous offrir des solutions fiables et durables, destinées à vous assister au cours des quatre phases du cycle de vie de l'ordinateur de bureau, à savoir la planification, la mise en œuvre, la supervision et les migrations.

Ce manuel résume les fonctionnalités et caractéristiques des sept éléments clés de la supervision des ordinateurs de bureau :

- Configuration et mise en œuvre initiales
- Installation de système à distance
- Mise à jour et gestion des logiciels
- Réécriture de la ROM
- Composantes et partenaires
- Suivi d'inventaire et sécurité
- Notification des pannes et récupération



La prise en charge des fonctions spécifiques décrites dans ce manuel peut varier selon les modèles ou la version du logiciel.

Configuration et mise en œuvre initiales

Les ordinateurs HP sont livrés avec un ensemble de logiciels système préinstallés. Après une courte opération de décompactage des logiciels, l'ordinateur est prêt à fonctionner.

Vous préférerez peut-être remplacer les logiciels préinstallés par un ensemble personnalisé de logiciels système et d'applications. Pour ce faire, vous disposez des méthodes suivantes:

- Installation d'applications logicielles supplémentaires après le décompactage de l'ensemble des logiciels préinstallés.
- Utilisation d'outils de déploiement, tels que Altiris eXpress, Microsoft MS Batch ou Microsoft NT Distribution Share (NTDS) pour remplacer les logiciels préinstallés par un ensemble personnalisé de logiciels.
- Application d'un procédé de clonage de disque permettant de copier le contenu d'un disque dur vers un autre.

La méthode de mise en œuvre la plus performante dépendra de votre environnement et de vos procédés informatiques. La section PC Deployment du site Internet Solutions and Services (à l'adresse <http://www.compaq.com/solutions/pcsolutions>) vous donne des informations quant à la méthode de déploiement optimale. Vous trouverez également des guides et des utilitaires pour intégrer les outils de déploiement Microsoft ou PXE.

Le CD *Compaq Restore* (ou *Restore Plus!*, l'utilitaire de configuration en ROM (RBSU) et le matériel compatible ACPI vous apportent une aide supplémentaire dans la récupération de logiciels système, la gestion de la configuration et la résolution des problèmes liés, ainsi que dans la gestion de l'alimentation.

Installation de système à distance

L'installation de système à distance vous permet de démarrer et de configurer votre système à partir des logiciels et des informations se trouvant sur un serveur réseau. La fonction d'installation à distance du système est généralement utilisée comme utilitaire d'installation et de configuration du système, et permet d'effectuer les tâches suivantes :

- Déploiement d'une image logicielle sur un ou plusieurs nouveaux PC.
- Formatage d'un disque dur.
- Installation de logiciels d'application ou de drivers.
- Mise à jour du système d'exploitation, des applications ou des drivers.

Pour lancer l'Installation de système à distance, appuyez sur **F12**, lorsque le message F12 = Network Service Boot (Démarrage des services réseau) apparaît dans l'angle inférieur droit de l'écran de logo HP. Suivez les instructions affichées à l'écran pour continuer l'opération.

HP et Altiris, Inc. se sont associés pour développer des outils permettant de faciliter et d'accélérer le déploiement et la gestion des PC en entreprise. Au final, ces outils permettront de diminuer le coût total d'exploitation et feront des PC HP les systèmes les plus faciles à gérer au sein de l'environnement d'entreprise.

Mise à jour et gestion des logiciels

HP offre plusieurs outils pour la gestion et la mise à jour des logiciels des ordinateurs de bureau et des stations de travail : Altiris eXpress, Altiris eXpress PC Transplant Pro, Altiris eXpress HP/Compaq Client Manager, System Software Manager, Product Change Notification et Active Update.

Altiris eXpress

HP et Altiris ont élargi leur partenariat pour offrir des solutions à la pointe de l'industrie qui réduisent la complexité de la supervision matérielle et logicielle des ordinateurs de bureau, des ordinateurs portables, des ordinateurs de poche et des serveurs tout au long de leur cycle de vie. Altiris eXpress permet à l'administrateur système de créer et de déployer rapidement une image personnalisée des logiciels de l'entreprise sur un ou plusieurs PC client en réseau avec une interface aussi conviviale que l'Explorateur Windows. Altiris eXpress prend en charge les spécifications Wired for Management et PXE (Preboot Execution Environment) d'Intel. L'utilisation conjointe d'Altiris eXpress et des fonctions d'installation de systèmes à distance de HP dispense l'administrateur système de déployer les logiciels sur chaque ordinateur personnel individuellement.

Les solutions d'Altiris eXpress permettent d'automatiser efficacement les processus existants et de résoudre les problèmes observés dans votre environnement informatique. Grâce à l'infrastructure Web d'Altiris eXpress, vous disposez désormais de la souplesse nécessaire pour superviser vos systèmes en tout lieu et à toute heure, même depuis votre iPAQ Pocket PC !

Les solutions d'Altiris eXpress sont modulaires et évolutives pour répondre à tous les besoins des groupes de travail de l'entreprise. Ils s'intègrent facilement aux autres outils de supervision clients et complètent Microsoft BackOffice/SMS.

Les solutions évoluées d'Altiris eXpress se concentrent sur quatre domaines clés de l'informatique :

- Déploiement et migration
- Gestion des logiciels et des opérations
- Gestion des stocks et des actifs
- Centre d'assistance et résolution des problèmes

En quelques minutes, Altiris eXpress peut installer une image disque contenant le système d'exploitation, des logiciels applicatifs et le client Altiris eXpress, sans nécessiter l'utilisation d'une disquette d'amorçage distincte. Grâce à Altiris eXpress, l'administrateur réseau peut :

- Créer une image ou en modifier une existante, ou encore cloner un PC du réseau qui possède l'image idéale.
- Créer un nombre quelconque d'images disque personnalisées pour différents groupes de travail.
- Éditer des fichiers image et les modifier sans avoir à recommencer depuis le début, grâce à la capacité de Altiris eXpress à stocker les fichiers dans son format natif : NTFS, FAT16 ou FAT32.
- Créer un script "New PC Event" (Événement Nouveau PC) qui s'exécutera automatiquement à chaque fois qu'un nouveau PC est ajouté au réseau. Le script peut, par exemple, formater le disque dur du PC, réécrire le BIOS ROM et installer une image logicielle standard complète.
- Programmer un événement pour qu'il s'exécute sur un groupe d'ordinateurs.

Altiris eXpress comprend également des fonctions de distribution de logiciels faciles d'emploi. Vous pouvez utiliser Altiris eXpress pour mettre à jour les systèmes d'exploitation et les applications depuis une console centrale. Utilisé conjointement avec System Software Manager, il est également en mesure de mettre à jour le BIOS ROM et les drivers de périphériques.

Pour plus d'informations, consultez le site
<http://www.compaq.com/easydeploy>.

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro permet une migration aisée en préservant les anciens paramètres, les préférences et les données et en les migrant rapidement et facilement vers le nouvel environnement. Les mises à niveau ne prennent plus des heures ou des jours, mais seulement quelques minutes, et l'ordinateur et les applications répondent exactement aux attentes des utilisateurs.

Pour télécharger une version d'évaluation entièrement fonctionnelle valable 30 jours, consultez le site <http://www.compaq.com/easydeploy>.

Altiris eXpress HP/Compaq Client Manager

Altiris eXpress HP/Compaq Client Manager intègre étroitement la technologie HP de Supervision intelligente dans Altiris eXpress pour offrir des fonctions avancées de supervision matérielle des périphériques d'accès HP. Il permet, entre autres :

- Des vues détaillées de l'inventaire matériel pour la gestion des actifs
- Un suivi de l'état du PC et des diagnostics
- Une notification proactive des modifications de l'environnement matériel
- Des rapports accessibles par le Web contenant des détails critiques pour l'entreprise comme, par exemple, des avertissements de surchauffe, des alertes mémoire, etc.
- La mise à niveau à distance des logiciels système, comme les drivers de périphériques et le BIOS de la mémoire morte.

Pour plus d'informations sur Altiris eXpress HP/Compaq Client Manager, consultez le site <http://www.compaq.com/easydeploy>.

System Software Manager

System Software Manager (SSM) est un utilitaire qui vous permet de mettre à jour simultanément les logiciels système de plusieurs PC. Exécuté sur un système PC client, SSM détecte à la fois les versions de logiciels et de périphériques matériels, puis met à niveau le logiciel voulu à partir d'un référentiel central (magasin de fichiers). Les versions des drivers prises en charge par SSM sont indiquées par une icône spéciale sur le site de téléchargement de drivers et sur le CD Support Software. Pour télécharger l'utilitaire ou pour plus d'informations sur SSM, visitez le site <http://www.compaq.com/im/ssmwp.html>.

Product Change Notification

PCN est le programme de notification de modification des produits HP qui utilise un site Web sécurisé dans lequel vous pouvez créer des profils personnalisés qui vous permettront, proactivement et automatiquement, de :

- Recevoir des avis électroniques de modification de matériel et de logiciels sur la plupart des ordinateurs et des serveurs professionnels.
- Recevoir des avis électroniques à la clientèle pour la plupart des ordinateurs et des serveurs professionnels.

Le site Web de PCN permet également aux utilisateurs de rechercher toutes les notifications de modification de produits et tous les avis à la clientèle pour la plupart des ordinateurs et des serveurs professionnels.

Pour en savoir plus à propos de PCN et pour créer votre profil personnalisé, visitez le site <http://www.compaq.com/pcn>.

ActiveUpdate

ActiveUpdate est une application cliente de HP. Le client ActiveUpdate est exécuté sur votre système local et utilise votre profil personnalisé pour télécharger proactivement et automatiquement les mises à jour logicielles pour la plupart des ordinateurs et des serveurs professionnels Compaq/HP.

Pour en savoir plus à propos de ActiveUpdate, télécharger l'application et créer votre profil personnalisé, visitez le site <http://www.compaq.com/activeupdate>.

Réécriture de la ROM

L'ordinateur dispose d'une mémoire morte (ROM) flash reprogrammable. En créant un mot de passe de configuration dans l'utilitaire Computer Setup (F10), vous pouvez protéger la mémoire morte contre toute mise à jour ou tout remplacement intempestif. Cela est important pour garantir l'intégrité opérationnelle de l'ordinateur. Si vous souhaitez mettre à niveau la mémoire morte, vous pouvez :

- commander à HP une disquette *ROMPaq*™ de mise à niveau ;
- télécharger les images ROMPaq les plus récentes à partir du site <http://www.compaq.com>.



ATTENTION : pour assurer une protection maximale de votre mémoire morte, n'oubliez pas de créer un mot de passe de configuration. Le mot de passe de configuration permet d'empêcher les mises à niveau non autorisées. L'utilitaire System Software Manager permet à l'administrateur système de définir un mot de passe sur un ou plusieurs PC en même temps. Pour plus d'informations, consultez le site <http://www.compaq.com/im/ssmwp.html>.

Réécriture de la ROM à distance

La fonction de réécriture de la ROM à distance permet à l'administrateur système de mettre à niveau en toute sécurité la ROM sur des ordinateurs HP distants, directement depuis la console de supervision réseau centralisée. Dans la mesure où l'administrateur système peut effectuer cette tâche à distance sur plusieurs ordinateurs, il obtient un déploiement cohérent et un meilleur contrôle sur les images ROM des PC HP du réseau. Il s'ensuit également une augmentation de la productivité et une diminution du coût d'exploitation.



L'ordinateur doit être en marche ou activé à l'aide de Réveil à distance (Remote Wakeup) pour pouvoir utiliser la réécriture de ROM à distance.

Pour de plus amples informations sur la mise à jour à distance de la ROM, veuillez consulter les rubriques Altiris eXpress HP/Compaq Client Manager ou System Software Manager du site Web Compaq EasyDeploy à l'adresse <http://www.compaq.com/easydeploy>.

Bloc d'amorçage ROM FailSafe

Le bloc d'amorçage ROM FailSafe permet de restaurer le système dans le cas improbable d'une panne pendant la réécriture de la ROM, par exemple si une coupure de courant se produisait pendant une mise à niveau de la ROM. Ce bloc d'amorçage est une section protégée en écriture qui contrôle la validité de réécriture de la ROM système chaque fois que le système est mis sous tension.

- Si la mémoire morte du système est valide, le système démarre normalement.
- Si le test de validité échoue, le bloc d'amorçage ROM FailSafe assure une prise en charge suffisante pour démarrer le système à partir d'une disquette ROMPaq, qui programmera une image valide pour la mémoire morte du système.

Si le bloc d'amorçage détecte une ROM système non valide, l'ordinateur émet une série de signaux sonores (un long et trois courts) et les trois voyants du clavier clignotent deux fois. Un message indiquant le passage au mode de récupération du bloc d'amorçage s'affiche alors à l'écran (sur certains modèles).

Pour restaurer le système après son passage au mode de récupération du bloc d'amorçage, procédez comme suit :


1. Retirez toute disquette se trouvant dans l'unité de disquette et éteignez l'ordinateur.
2. Insérez une disquette ROMPaq dans l'unité de disquette.
3. Mettez le système sous tension.
4. Si aucune disquette ROMPaq n'est détectée, vous devrez en insérer une et redémarrer l'ordinateur.
5. Si vous avez défini un mot de passe de configuration, le voyant Verr Maj s'allume et un message vous demande d'entrer votre mot de passe.
6. Saisissez votre mot de passe de configuration.
7. Si le système démarre à partir de la disquette et reprogramme la mémoire morte avec succès, les trois voyants du clavier s'allument. Une série de signaux sonores de plus en plus aigus indique le succès de l'opération.

Pour vous assurer que la réécriture de la ROM a réussi, effectuez les étapes suivantes :

1. Insérez une disquette ROMPaq valide dans l'unité de disquette.
2. Mettez le système hors tension.
3. Mettez l'ordinateur sous tension pour réécrire à nouveau la mémoire morte.
4. Si la réécriture de la ROM a réussi, les trois voyants du clavier s'allument et vous entendez une série de signaux sonores de plus en plus aigus.
5. Retirez la disquette et mettez l'ordinateur hors tension, puis sous tension pour le redémarrer.

Le tableau suivant donne la liste des différentes combinaisons de voyants utilisées par le bloc d'amorçage ROM, ainsi que leur signification et les opérations à effectuer selon la combinaison.

Combinaisons des voyants du clavier utilisées par le bloc d'amorçage ROM

Mode Bloc d'amorçage Failsafe	Couleur du voyant du clavier	Activité des voyants du clavier	État/Message
Verr num	Vert	Allumé	La disquette ROMPaq est absente, défectueuse ou l'unité n'est pas prête.*
Verr maj	Vert	Allumé	Saisissez votre mot de passe.*
Verr num, Maj, Arrêt défil	Verts	S'allument et s'éteignent deux fois (avec 1 signal sonore long et 3 courts)	Échec de la réécriture de la ROM.*
Verr num, Maj, Arrêt défil	Verts	Allumés	Réussite de la réécriture de la ROM du bloc d'amorçage. Éteignez, puis rallumez l'ordinateur pour le relancer.
 Les voyants de diagnostic ne clignotent pas sur les claviers USB.			

Réplication de la configuration

Cette opération permet à un administrateur de copier facilement la configuration d'un ordinateur sur d'autres ordinateurs du même modèle. Ceci permet une configuration plus rapide et plus cohérente de plusieurs ordinateurs. Pour répliquer votre configuration :

1. Accédez au menu de l'utilitaire Computer Setup (F10).
2. Cliquez sur **File > Save to Diskette (Fichier > Enregistrer sur disquette)**. Suivez les instructions s'affichant à l'écran.



Cette procédure nécessite une unité de disquette interne ou une unité de disquette externe.

3. Pour répliquer la configuration, cliquez sur **File File > Restore from Diskette, (Fichier > Restaurer à partir de la disquette)** et suivez les instructions à l'écran.

Altiris eXpress, System Software Manager et PC Transplant permettent de répliquer facilement la configuration et les paramètres personnalisés d'un PC, puis de les copier sur un ou plusieurs PC. Pour plus d'informations à ce sujet, consultez le site

<http://www.compaq.com/easydeploy>.

Bouton d'alimentation double état

Lorsque l'interface ACPI (Advanced Configuration and Power Interface) est activée sous Windows 98, Windows 2000, Windows Millennium ou Windows XP, le bouton de mise sous tension peut servir d'interrupteur Marche/Arrêt ou de bouton d'activation du mode Suspend. La fonction Suspend ne met pas l'appareil hors tension, mais le fait passer en mode Veille où sa consommation électrique est minimale. Cela vous permet d'arrêter le système sans fermer les applications et de reprendre rapidement votre travail où vous l'aviez laissé sans perdre de données.

Pour changer la configuration du bouton de mise sous tension, procédez comme suit :

1. Dans Windows 2000, cliquez sur **Démarrer**, puis pointez sur **Paramètres > Panneau de configuration > Options d'alimentation**.

Dans Windows XP, cliquez sur **Démarrer**, puis sélectionnez **Panneau de configuration > Performances et maintenance > Options d'alimentation**.

2. Dans la fenêtre **Propriétés de Options d'alimentation**, sélectionnez l'onglet **Paramètres avancés**.
3. Dans le volet Boutons d'alimentation, sélectionnez la configuration de votre choix pour le bouton de mise sous tension.

Si vous avez configuré le bouton d'alimentation en mode Suspend, le fait d'appuyer brièvement dessus fait passer l'ordinateur dans un état à très faible consommation. En appuyant à nouveau sur le bouton, vous ramenez le fonctionnement du système à pleine puissance. Pour couper complètement l'alimentation de l'ordinateur, appuyez sur le bouton de mise sous tension pendant quatre secondes.

Gestion de l'alimentation

Cette fonction permet d'arrêter certains composants de l'ordinateur lorsqu'ils ne sont pas utilisés, et contribue aussi à économiser de l'énergie, sans arrêter l'ordinateur.

Sous Windows 98, Windows 2000, Windows Millennium et Windows XP, lorsque Advanced Configuration et Power Interface (ACPI) est activé, les délais d'attente (temps d'inactivité admis avant d'arrêter ces composants) peuvent être activés, personnalisés ou désactivés à l'aide du système d'exploitation.

1. Dans Windows 2000, cliquez sur **Démarrer**, puis pointez sur **Paramètres > Panneau de configuration > Options d'alimentation**.
Dans Windows XP, cliquez sur **Démarrer**, puis sélectionnez **Panneau de configuration > Performances et maintenance > Options d'alimentation**.
2. Dans la fenêtre **Propriétés de Options d'alimentation**, sélectionnez l'onglet **Modes de gestion de l'alimentation**.
3. Sélectionnez les paramètres de votre choix pour le mode de gestion de l'alimentation.

Utilisez Propriétés de l'affichage pour définir, modifier ou désactiver les fonctions de gestion de l'alimentation du moniteur. Pour accéder aux Propriétés de l'affichage, cliquez avec le bouton droit sur le **Bureau Windows**, puis choisissez **Propriétés**.

Site Web

Les ingénieurs HP ont procédé à des tests rigoureux et au débogage des logiciels mis au point par HP et d'autres éditeurs. Ils ont également développé un logiciel spécifique de prise en charge de système d'exploitation afin de garantir le plus haut niveau de performances, de compatibilité et de fiabilité pour les ordinateurs HP.

Lorsque vous installez des systèmes d'exploitation nouveaux ou révisés, il est important d'exécuter le logiciel de prise en charge conçu pour ce système d'exploitation. Si vous prévoyez d'utiliser une version de Microsoft Windows différente de celle fournie avec votre ordinateur, vous devez installer les drivers de périphériques et les utilitaires appropriés afin de garantir la prise en charge correcte et l'exécution de toutes les fonctionnalités.

HP a simplifié la localisation, l'accès, l'évaluation et l'installation des logiciels de support appropriés. Vous pouvez télécharger ces logiciels à partir du site <http://www.compaq.com>.

Ce site contient les derniers drivers de périphériques, utilitaires et images de réécriture ROM dont vous avez besoin pour exécuter le système d'exploitation Microsoft Windows le plus récent sur votre ordinateur HP.

Composantes et partenaires

Les solutions de supervision HP s'appuient sur les normes établies, telles que DMI 2.0, WBEM (Web-Based Enterprise Management), WfM (Wired for Management) d'Intel, SNMP et les technologies PXE (preboot execution environment). Microsoft, Intel, Altiris et d'autres fabricants à la pointe de l'industrie travaillent en étroite collaboration avec HP pour intégrer leurs solutions de supervision dans les produits et initiatives HP afin d'offrir les meilleures solutions de supervision intelligente aux utilisateurs de PC. Pour plus d'informations, consultez le site <http://www.compaq.com/easydeploy>.

Desktop Management Interface (DMI)

L'association DMTF (Desktop Management Task Force) est un organisme professionnel créé en 1992, dont l'objectif est de standardiser la supervision de systèmes. DMTF a créé l'interface DMI afin de normaliser l'accès aux données de configuration des PC. En tant que membre du comité directeur et du comité technique du DMTF, HP fournit du matériel et des logiciels qui prennent en charge la norme DMI.

Pour savoir comment configurer le logiciel DMI, reportez-vous au fichier d'aide du guide *Intelligent Manageability Guide* (Supervision intelligente).

Wired for Management

L'initiative d'Intel Wired for Management (WfM) a pour objectif la réduction des coûts de support et d'administration des systèmes à architecture Intel sans nuire à leur souplesse ni à leurs performances. Les directives Wired for Management fournissent un ensemble de modules de base que HP utilise dans la supervision intelligente pour fournir une gestion standardisée des inventaires, pour la configuration à distance, pour la maintenance en dehors des heures d'exploitation et pour la gestion d'énergie de la nouvelle génération. Mais HP va encore plus loin. La Supervision intelligente est pourvue de fonctionnalités supplémentaires fournissant une solution globale de supervision adaptée aux environnements réseaux.

La technologie Wired for Management comprend :

- Interface de gestion d'ordinateurs de bureau (DMI) 2.0
- Installation de système à distance
- Réveil et arrêt à distance
- Matériel compatible ACPI
- SMBIOS
- Prise en charge de PXE (Pre-boot Execution)

Suivi d'inventaire et sécurité

Les fonctions AssetControl Compaq intégrées à l'ordinateur fournissent les données principales de suivi d'inventaire qui peuvent être supervisées à l'aide des produits HP Insight Manager et ceux des Partenaires Solutions de supervision. L'intégration automatique qui se fait en continu entre les fonctions AssetControl et ces produits vous permet de choisir l'outil de gestion le mieux adapté à votre environnement et d'exploiter vos outils existants.

Les ordinateurs de bureau HP sont fabriqués avec des composants matériels et logiciels assurant une prise en charge complète de la norme DMI 2.0.

HP propose en outre différentes solutions permettant de sécuriser l'accès aux éléments et aux données essentiels de l'ordinateur. Les fonctions de sécurité, telles que le capteur Smart Cover et le verrou Smart Cover disponibles sur certains modèles, empêchent tout accès non autorisé aux composants internes de l'ordinateur. En désactivant les ports parallèles, de série ou USB ou en désactivant la capacité d'amorçage sur supports amovibles, vous pouvez protéger vos données importantes. Les alertes de modification de mémoire et de capteur Smart Cover peuvent être transmises automatiquement aux produits HP Insight Manager, afin d'émettre des messages proactifs en cas de manipulation des composants internes de l'ordinateur.



Le capteur Smart Cover et le verrou Smart Cover sont disponibles en option sur certains systèmes.

Vous pouvez gérer les paramètres de sécurité de votre ordinateur HP à l'aide des utilitaires suivants :

- Localement, avec l'utilitaire Computer Setup. Pour en savoir plus et obtenir des instructions sur l'utilisation de Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)* fourni avec l'ordinateur.
- À distance à l'aide de System Software Manager. Ce logiciel permet le déploiement sûr et cohérent, ainsi que le contrôle des paramètres de sécurité à partir d'un simple utilitaire à ligne de commandes.

Les sections et le tableau suivants décrivent les fonctions locales de supervision de la sécurité de votre ordinateur offertes par l'utilitaire Computer Setup (F10).

Présentation des fonctions de sécurité

Fonction	Action	Mise en place
Contrôle d'amorçage sur support amovible	Empêche le démarrage à partir d'unités amovibles.	À partir du menu de l'utilitaire Computer Setup (F10).
Contrôle des interfaces série, parallèle, USB ou infrarouge	Empêche la transmission de données par l'intermédiaire de l'interface série, parallèle, USB (universal serial bus) ou infrarouge intégrée.	À partir du menu de l'utilitaire Computer Setup (F10).
Power-On Password (Mot de passe de mise sous tension)	Interdit l'utilisation de l'ordinateur jusqu'à la saisie du mot de passe. Cela peut s'appliquer à la fois au démarrage initial et au redémarrage du système.	À partir du menu de l'utilitaire Computer Setup (F10).
Mot de passe de configuration	Empêche la reconfiguration de l'ordinateur (utilisation de Computer Setup) tant que le mot de passe n'a pas été saisi.	À partir du menu de l'utilitaire Computer Setup (F10).
Mode Serveur réseau	Fournit des fonctions de sécurité uniques destinées aux ordinateurs utilisés en tant que serveurs.	À partir du menu de l'utilitaire Computer Setup (F10).
DriveLock	Empêche tout accès non autorisé aux données stockées sur des disques durs donnés. Cette fonctionnalité n'est disponible que sur certains modèles.	À partir du menu de l'utilitaire Computer Setup (F10).

Présentation des fonctions de sécurité (Suite)

Fonction	Action	Mise en place
Détecteur Smart Cover	Signale que le capot ou le panneau latéral de l'ordinateur a été retiré. Peut être réglé pour demander la saisie du mot de passe de configuration avant le redémarrage de l'ordinateur, après que le capot ou le panneau latéral a été retiré. Pour plus d'informations sur cette fonction, reportez-vous au <i>Manuel de référence du matériel</i> figurant sur le CD <i>Documentation Library</i> .	À partir du menu de l'utilitaire Computer Setup (F10).
Master Boot Record Security	Peut empêcher la modification accidentelle ou malveillante du secteur d'amorçage principal (MBR) du disque amorçable actuel et permet de restaurer le dernier MBR correct connu.	À partir du menu de l'utilitaire Computer Setup (F10).
Alertes de modification de mémoire	Détectent l'ajout, le déplacement ou le retrait de modules mémoire, et en avertit l'utilisateur et l'administrateur système.	Pour plus d'informations sur l'activation des alertes de modification de mémoire, reportez-vous au guide en ligne <i>Intelligent Manageability (Supervision intelligente)</i> .
Étiquette de propriétaire	Affiche les informations de propriété, définies par l'administrateur lors de l'installation du système (protégé par le mot de passe de configuration).	À partir du menu de l'utilitaire Computer Setup (F10).

Présentation des fonctions de sécurité (Suite)

Fonction	Action	Mise en place
Dispositif antivol	Bloque l'accès à l'intérieur de l'ordinateur pour empêcher un changement intempestif de la configuration ou le retrait de composants. Permet également d'attacher l'ordinateur à un objet fixe pour le protéger contre le vol.	Installez un dispositif antivol pour attacher l'ordinateur à un objet fixe.
Boucle antivol	Bloque l'accès à l'intérieur de l'ordinateur pour empêcher un changement intempestif de la configuration ou le retrait de composants.	Installez un verrou dans la boucle de sécurité pour empêcher tout changement indésirable de configuration ou retrait de composant.



Pour des instructions sur Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)*. La prise en charge des options de sécurité peut varier en fonction de la configuration de votre ordinateur.

Sécurité par mot de passe

Le mot de passe de mise sous tension empêche l'accès non autorisé à votre ordinateur en demandant la saisie d'un mot de passe pour accéder aux applications ou aux données, chaque fois que l'ordinateur est allumé ou redémarré. Le mot de passe de configuration empêche l'accès non autorisé à Computer Setup et peut aussi être utilisé à la place du mot de passe de mise sous tension. Cela signifie que lorsque l'invite de saisie du mot de passe de mise sous tension s'affiche, vous pouvez saisir le mot de passe de configuration pour accéder à l'ordinateur.

La création d'un mot de passe de configuration à l'échelle du réseau est aussi possible, ce qui permet à l'administrateur système d'accéder à tous les systèmes du réseau pour effectuer des opérations de maintenance sans avoir besoin de connaître votre mot de passe de mise sous tension, même si celui-ci a été défini.

Création d'un mot de passe de configuration à l'aide de Computer Setup

La création d'un mot de passe de configuration par le biais de l'utilitaire Computer Setup (F10) empêche la reconfiguration de votre ordinateur, à l'aide de ce même utilitaire, tant que le mot de passe n'a pas été saisi.

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur Démarrer **Arrêter** > **Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 Setup apparaît dans l'angle inférieur droit de l'écran. Appuyez sur **Entrée** pour ignorer l'écran de titre, le cas échéant.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Sélectionnez **Sécurité**, puis **Mot de passe de configuration** et suivez les instructions qui s'affichent.
4. Avant de quitter, cliquez sur **File** > **Save Changes and Exit**. (**Fichier** > **Enregistrer les modifications et Quitter**).

Création d'un mot de passe de démarrage à l'aide de Computer Setup

La création d'un mot de passe de mise sous tension par le biais de l'utilitaire Computer Setup bloque l'accès à l'ordinateur, lors de sa mise sous tension, jusqu'à la saisie du mot de passe. Lorsqu'un mot de passe de mise sous tension est défini, Computer Setup propose des options de mot de passe (Password Options) dans le menu Security. Ces options comprennent le mode Serveur réseau (Network Server Mode) et l'invite de mot de passe lors du redémarrage à chaud (Password Prompt on Warm Boot).

Si le mode Serveur réseau est désactivé, le mot de passe doit être saisi chaque fois que l'ordinateur est mis sous tension lorsque l'icône en forme de clé s'affiche sur le moniteur. Si l'option d'invite de mot de passe au redémarrage (Password Prompt on Warm Boot) est activée, le mot de passe doit également être entré lors du redémarrage de l'ordinateur. Lorsque le mode Serveur réseau est activé, l'invite de mot de passe n'apparaît pas pendant l'auto-test de mise sous tension (POST), mais tout clavier PS/2 relié à l'ordinateur reste bloqué tant que l'utilisateur n'a pas entré le mot de passe de mise sous tension.

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 Setup apparaît dans l'angle inférieur droit de l'écran. Appuyez sur **Entrée** pour ignorer l'écran de titre, le cas échéant.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Sélectionnez **Sécurité**, puis **Mot de passe de configuration** et suivez les instructions qui s'affichent.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit**. (**Fichier > Enregistrer les modifications et Quitter**).

Saisie d'un mot de passe de mise sous tension

Pour saisir un mot de passe de mise sous tension, procédez comme suit :

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Lorsque l'icône en forme de clé apparaît à l'écran, saisissez le mot de passe actuel, puis appuyez sur **Entrée**.



Entrez le mot de passe avec soin. Pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.

Si vous saisissez le mot de passe de manière incorrecte, une icône représentant une clé brisée apparaît à l'écran. Essayez une nouvelle fois. Après trois tentatives infructueuses, vous devrez éteindre l'ordinateur, puis le remettre en marche avant de pouvoir continuer.

Saisie du mot de passe de configuration

Si un mot de passe de configuration a été défini sur l'ordinateur, un message vous demande de l'entrer à chaque exécution de l'utilitaire Computer Setup.

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 = Setup apparaît dans l'angle inférieur droit de l'écran.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Lorsque l'icône en forme de clé apparaît à l'écran, saisissez le mot de passe de configuration, puis appuyez sur la touche **Enter**.



Entrez le mot de passe avec soin. Pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.

Si vous saisissez le mot de passe de manière incorrecte, une icône représentant une clé brisée apparaît à l'écran. Essayez une nouvelle fois. Après trois tentatives infructueuses, vous devrez éteindre l'ordinateur, puis le remettre en marche avant de pouvoir continuer.

Changement d'un mot de passe de mise sous tension ou de configuration

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer Arrêter > Redémarrer l'ordinateur**. Pour modifier le mot de passe de configuration, exécutez **Computer Setup**.
2. Lorsque l'icône en forme de clé apparaît, saisissez votre mot de passe actuel, le caractère de séparation approprié, votre nouveau mot de passe, le caractère de séparation approprié, et encore une fois votre nouveau mot de passe, selon le schéma suivant :
mot de passe courant!nouveau mot de passe!nouveau mot de passe



Entrez le mot de passe avec soin. Pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.

3. Appuyez sur la touche **Enter**.

Le nouveau mot de passe entre en vigueur à la mise sous tension de l'ordinateur qui suit.



Veillez vous référer à la rubrique “Caractères de séparation selon les claviers” pour connaître les caractères de séparation à utiliser. Le mot de passe de mise sous tension et celui de configuration peuvent aussi être modifiés à l’aide des options de Sécurité dans Computer Setup.

Suppression d'un mot de passe de mise sous tension ou de configuration

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur Démarrer **Arrêter** > **Redémarrer l'ordinateur**. Pour modifier le mot de passe de configuration, exécutez **Computer Setup**.
2. Lorsque l'icône Clé apparaît, saisissez votre mot de passe courant, suivi du caractère de séparation approprié, comme suit :
mot de passe courant!
3. Appuyez sur la touche **Enter**.



Veillez vous reporter à la section “Caractères de séparation selon les claviers” pour connaître les caractères de séparation à utiliser. Le mot de passe de mise sous tension et celui de configuration peuvent aussi être modifiés à l’aide des options de Sécurité dans Computer Setup.

Caractères de séparation selon les claviers

Chaque clavier est conçu pour répondre aux besoins spécifiques d'un pays. La syntaxe et les touches que vous utilisez pour changer ou supprimer un mot de passe dépendent du clavier utilisé avec l'ordinateur.

Caractères de séparation selon les claviers

Arabe	/	Grec	–	Russe	/
Belge	=	Hébreu	.	Slovaque	–
BHCSY*	–	Hongrois	–	Espagnol	–
Brésilien	/	Italien	–	Suédois/Finnois	/
Chinois	/	Japonais	/	Suisse	–
Tchèque	–	Coréen	/	Taïwanais	/
Danois	–	Latino-américain	–	Thaïlandais	/
Français	!	Norvégien	–	Turc	.
Français (Canada)	é	Polonais	–	Anglais (RU)	/
Allemand	–	Portugais	–	Anglais (USA)	/

* Pour Bosnie-Herzégovine, Croatie, Slovénie et Yougoslavie

Annulation des mots de passe

Si vous oubliez votre mot de passe, vous ne pouvez pas accéder à l'ordinateur. Reportez-vous au *Manuel de résolution des problèmes* pour savoir comment effacer des mots de passe.

Mode Serveur réseau

Le mode Serveur réseau fournit des fonctions de sécurité uniques destinées aux ordinateurs utilisés comme serveurs. Il est disponible uniquement lorsqu'un mot de passe de mise sous tension a été défini dans Computer Setup. Lorsque le mode Serveur réseau est activé, le mot de passe de mise sous tension n'est pas nécessaire pour amorcer le disque dur et un clavier ne doit pas obligatoirement être raccordé au système. Si un clavier PS/2 est présent, il est bloqué jusqu'à ce que l'utilisateur entre le mot de passe de mise sous tension. S'il s'agit d'un clavier USB, il reste utilisable par défaut. Pour empêcher l'accès au clavier USB après le chargement du système d'exploitation, l'utilisateur doit masquer le port USB dans l'option Device Security (Sécurité des unités) du menu Security (Sécurité) de l'utilitaire Computer Setup. Utilisé conjointement avec l'option de mise sous tension After Power Loss (Après défaillance de l'alimentation) de Computer Setup, le mode Serveur réseau permet au "serveur" de redémarrer automatiquement après une coupure de l'alimentation, sans intervention de l'utilisateur. Lorsque le mode Serveur réseau est activé, il est nécessaire d'entrer le mot de passe de mise sous tension pour amorcer les supports amovibles (disquettes) ou les périphériques amovibles (comme les périphériques flash USB).

DriveLock

DriveLock est une fonction de sécurité qui empêche tout accès non autorisé aux données stockées sur des disques durs spécifiques. DriveLock a été implémenté comme une extension de Computer Setup. Cette fonction n'est disponible que sur certains systèmes et uniquement lorsque des disques durs prenant en charge DriveLock sont détectés.

DriveLock s'adresse aux clients de HP pour lesquels la sécurité des données revêt une importance capitale. Pour eux, le coût du disque dur et la perte des données qu'il contient sont futiles par rapport au drame que représenterait l'accès non autorisé à ces données. Pour établir un compromis entre ce niveau de sécurité extrême et la nécessité de pouvoir remplacer un mot de passe oublié, DriveLock utilise un schéma de sécurité à deux mots de passe. L'un d'eux est défini et utilisé par l'administrateur du système tandis que l'autre est généralement défini et employé par l'utilisateur final. Si ces deux mots de passe sont oubliés, il n'y a plus aucun moyen de débloquent le disque. C'est pourquoi il est plus sûr d'utiliser DriveLock lorsque les données stockées sur le disque dur sont répliquées sur un système général d'entreprise ou régulièrement sauvegardées.

En cas de perte des deux mots de passe utilisés par DriveLock, le disque dur est inutilisable. Les utilisateurs qui ne correspondent pas au profil défini plus haut ne peuvent pas se permettre de prendre ce risque. En revanche, les clients qui présentent ce profil ne courent pas un gros danger compte tenu de la nature des données stockées sur le disque dur.

Utilisation de DriveLock

L'option DriveLock fait partie du menu Security de l'utilitaire Computer Setup. L'utilisateur peut choisir de définir le mot de passe principal ou d'activer DriveLock. Pour activer DriveLock, vous devez fournir un mot de passe d'utilisateur. Dans la mesure où la configuration initiale de DriveLock est généralement effectuée par un administrateur système, il convient de commencer par définir le mot de passe principal. HP encourage les administrateurs système à définir un mot de passe principal, qu'ils envisagent ou non d'activer DriveLock. De cette manière, si le disque dur venait à être verrouillé, l'administrateur serait en mesure de modifier les paramètres de DriveLock. Une fois le mot de passe principal défini, l'administrateur système peut activer DriveLock ou laisser cette option désactivée.

Si le disque dur est verrouillé, l'auto-test de mise sous tension (POST) exige un mot de passe pour le déverrouiller. Si un mot de passe de mise sous tension est défini et s'il correspond au mot de passe d'utilisateur, POST n'invite pas l'utilisateur à entrer une seconde fois son mot de passe. Dans le cas contraire, l'utilisateur est invité à entrer un mot de passe DriveLock. Il peut utiliser le mot de passe principal ou le mot de passe d'utilisateur. Le nombre de tentatives est limité à deux. Si toutes deux échouent, le POST continue, mais les données stockées sur le disque restent inaccessibles.

Applications de DriveLock

La fonction de sécurité DriveLock est surtout utilisée dans les entreprises où un administrateur système fournit aux utilisateurs des disques durs Multibay utilisables sur certains ordinateurs. L'administrateur système est responsable de la configuration du disque dur MultiBay, qui comprend notamment la définition du mot de passe DriveLock principal. Si l'utilisateur oublie son mot de passe ou si un autre employé récupère l'équipement, le mot de passe principal permet de redéfinir le mot de passe d'utilisateur et d'accéder à nouveau au disque dur.

HP recommande aux administrateurs système d'entreprise qui choisissent d'activer DriveLock de mettre au point une stratégie commune pour la définition et la gestion des mots de passe principaux. Cela permet d'éviter les situations où un employé définit les deux mots de passe DriveLock (intentionnellement ou non) avant de quitter l'entreprise. Dans un tel scénario, le disque dur devient inutilisable et doit être remplacé. De même, s'ils ne définissent pas de mot de passe principal, les administrateurs système risquent de se retrouver dans l'incapacité d'accéder à un disque dur afin d'y effectuer les opérations d'administration habituelles, notamment de vérifier qu'il ne contient pas de logiciels non autorisés, et de procéder au contrôle d'inventaire et à la maintenance.


HP recommande aux utilisateurs dont les contraintes de sécurité sont moins sévères de ne pas activer DriveLock. Il s'agit notamment des particuliers ou des employés qui ne gèrent pas de données confidentielles sur leur disque dur. Pour ces personnes, la perte d'un disque dur due à l'oubli des deux mots de passe est bien plus grave comparée à la valeur des données. L'accès à Computer Setup et à DriveLock peut être limité à l'aide d'un mot de passe de configuration. En spécifiant un mot de passe de configuration qu'il ne communique pas aux utilisateurs, l'administrateur peut empêcher ces derniers d'activer DriveLock.

Détecteur Smart Cover

Disponible sur certains modèles seulement, le détecteur Smart Cover est une combinaison de technologie matérielle et logicielle qui vous avertit lorsque le capot ou le panneau latéral de l'ordinateur est retiré. Il existe trois niveaux de protection, décrits dans le tableau suivant :

Niveaux de protection du détecteur Smart Cover

Niveau	Paramètre	Description
Niveau 0	Désactivé	Le capteur Smart Cover est inactif (par défaut).
Niveau 1	Avertir utilisateur	Au redémarrage de l'ordinateur, affichage d'un message signalant que le capot ou que le panneau latéral de l'ordinateur a été retiré.
Niveau 2	Mot de passe de configuration	Au redémarrage de l'ordinateur, affichage d'un message signalant que le capot ou que le panneau latéral de l'ordinateur a été retiré. Vous devez saisir votre mot de passe de configuration pour pouvoir continuer.

 Ces paramètres peuvent être modifiés à l'aide de Computer Setup. Pour plus d'informations sur Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)*.

Configuration du niveau de protection du détecteur Smart Cover

Pour définir le niveau de protection du détecteur Smart Cover, procédez comme suit :

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur Démarrer **Arrêter** > **Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 Setup apparaît dans l'angle inférieur droit de l'écran. Appuyez sur **Entrée** pour ignorer l'écran de titre, le cas échéant.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Sélectionnez **Security (Sécurité)**, puis **Smart Cover**, et suivez les instructions qui s'affichent.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit.** (**Fichier > Enregistrer les modifications et Quitter**).

Verrou Smart Cover

Le verrou Smart Cover est un dispositif de verrouillage contrôlé par logiciel, présent sur certains ordinateurs HP. Ce système empêche tout accès non autorisé aux composants internes de l'ordinateur. Les ordinateurs sont livrés avec le verrou en position déverrouillée.



ATTENTION : pour obtenir une sécurité optimale de verrouillage du capot, créez un mot de passe de configuration. En effet, celui-ci permet d'empêcher l'accès non autorisé à l'utilitaire Computer Setup.



Le verrou Smart Cover est disponible en option sur certains systèmes.

Mise en place du verrou Smart Cover

Pour activer et verrouiller le verrou Smart Cover, procédez comme suit :

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur Démarrer **Arrêter** > **Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 Setup apparaît dans l'angle inférieur droit de l'écran. Appuyez sur **Entrée** pour ignorer l'écran de titre, le cas échéant.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Sélectionnez **Security (Sécurité)**, puis **Smart Cover**, et l'option **Locked (Verrouillé)**.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit.** (**Fichier > Enregistrer les modifications et Quitter**).

Déblocage du verrou Smart Cover

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur Démarrer **Arrêter** > **Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 Setup apparaît dans l'angle inférieur droit de l'écran. Appuyez sur **Entrée** pour ignorer l'écran de titre, le cas échéant.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Sélectionnez **Security > Smart Cover > Unlocked.**
4. Avant de quitter, cliquez sur **File > Save Changes and Exit.** (**Fichier > Enregistrer les modifications et Quitter**).

Utilisation de la clé Smart Cover FailSafe

Si vous activez le verrou Smart Cover et que vous ne pouvez pas entrer le mot de passe pour le désactiver, vous aurez besoin d'une clé Smart Cover FailSafe pour ouvrir le capot de l'ordinateur. Cette clé vous sera également nécessaire dans les cas suivants :

- Coupure de courant
- Panne au démarrage
- Défaillance d'un composant (processeur ou alimentation, par exemple)
- Oubli de mot de passe



ATTENTION : la clé Smart Cover FailSafe est un outil spécialisé fourni par HP. Pour parer à toute éventualité, commandez cette clé avant d'avoir à vous en servir auprès d'un revendeur ou mainteneur agréé (référence PN 166527-001 pour la clé ou PN 166527-002 pour le type tournevis).

Vous pouvez vous procurer la clé FailSafe suivant une des procédures ci-dessous :

- Contactez votre revendeur ou mainteneur agréé HP.
- Pour les informations de commande, consultez le site <http://www.compaq.com>.
- Consultez la liste des numéros de téléphone dans la garantie pour appeler le numéro approprié.

Pour en savoir plus sur l'utilisation de la clé Smart Cover FailSafe, consultez le *Manuel de référence du matériel*.

Sécurité MBR (Master Boot Record)

Le MBR contient les informations nécessaires pour démarrer le système à partir d'un disque et accéder aux données stockées sur ce dernier. La sécurité MBR évite les modifications accidentelles ou malveillantes du MBR, comme celles provoquées par certains virus informatiques ou par l'utilisation erronée de certains utilitaires de disque. Elle permet également de restaurer le dernier MBR "fiable" au cas où des modifications du MBR seraient détectées au redémarrage du système.

Pour activer la sécurité MBR, procédez comme suit :

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 Setup apparaît dans l'angle inférieur droit de l'écran. Appuyez sur **Entrée** pour ignorer l'écran de titre, le cas échéant.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Sélectionnez **Security (Sécurité) > Master Boot Record Security > Enabled (Activée)**.
4. Sélectionnez **Security (Sécurité) > Save Master Boot Record (Enregistrement du MBR)**.
5. Avant de quitter, cliquez sur **File > Save Changes and Exit. (Fichier > Enregistrer les modifications et Quitter)**.

Lorsque la sécurité MBR est activée, le BIOS empêche toute modification du MBR du disque amorçable en cours en mode MS-DOS ou Windows Sans échec.



La plupart des systèmes d'exploitation contrôlent l'accès au MBR du disque amorçable en cours et, par conséquent, le BIOS ne peut empêcher l'ajout de modifications lorsque le système d'exploitation s'exécute.

À chaque mise sous tension ou redémarrage de l'ordinateur, le BIOS compare le MBR du disque amorçable actuel au MBR précédemment enregistré. Si des modifications sont détectées et si le disque amorçable actuel est celui à partir duquel le MBR a été précédemment enregistré, le message suivant s'affiche :

1999 – Master Boot Record has changed (Le MBR a été modifié).

Press any key to enter Setup to configure MBR Security
(Appuyez sur n'importe quelle touche pour accéder au programme Computer Setup et configurer la sécurité MBR).

Dans l'utilitaire Computer Setup, vous devez :

- enregistrer le MBR du disque amorçable actuel,
- restaurer le MBR précédemment enregistré, ou
- désactiver la fonction de sécurité MBR.

Vous devez connaître le mot de passe de configuration, s'il a été défini.

Si des modifications sont détectées et si le disque amorçable actuel **n'est pas** le disque à partir duquel le MBR a été précédemment enregistré, le message suivant s'affiche :

2000 – Master Boot Record Hard Drive has changed (Le disque dur du MBR a changé).

Press any key to enter Setup to configure MBR Security
(Appuyez sur n'importe quelle touche pour accéder au programme Computer Setup et configurer la sécurité MBR).

Dans l'utilitaire Computer Setup, vous devez :

- enregistrer le MBR du disque amorçable actuel, ou
- désactiver la fonction de sécurité MBR.

Vous devez connaître le mot de passe de configuration, s'il a été défini.

Dans le cas peu probable où le MBR précédemment enregistré aurait été altéré, le message suivant s'affiche :

1998 – Master Boot Record has been lost (Perte du MBR).

Press any key to enter Setup to configure MBR Security
(Appuyez sur n'importe quelle touche pour accéder au programme Computer Setup et configurer la sécurité MBR.

Dans l'utilitaire Computer Setup, vous devez :

- enregistrer le MBR du disque amovible actuel, ou
- désactiver la fonction de sécurité MBR.

Vous devez connaître le mot de passe de configuration, s'il a été défini.

Avant de partitionner ou de formater le disque amovible actuel

Assurez-vous que la sécurité MBR est désactivée avant de modifier le partitionnement ou le formatage du disque amovible actuel. Divers utilitaires de disque comme FDISK et FORMAT tentent de mettre à jour le MBR. Si la sécurité MBR est activée lorsque vous modifiez le partitionnement ou le formatage du disque, il se peut que vous receviez des messages d'erreur de l'utilitaire de disque ou un avertissement de la sécurité MBR lors de la prochaine mise sous tension de l'ordinateur ou de son redémarrage. Pour désactiver la sécurité MBR, procédez comme suit :

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur Démarrer **Arrêter** > **Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le message F10 Setup apparaît dans l'angle inférieur droit de l'écran. Appuyez sur **Entrée** pour ignorer l'écran de titre, le cas échéant.



Si vous n'appuyez pas sur la touche **F10** lorsque le message s'affiche, vous devrez redémarrer l'ordinateur pour avoir accès à l'utilitaire.

3. Sélectionnez **Security (Sécurité) > Master Boot Record Security > Disabled (Désactivée)**.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit. (Fichier > Enregistrer les modifications et Quitter)**.

Dispositif antivol

Le panneau arrière de l'ordinateur est prévu pour recevoir un dispositif antivol permettant d'attacher physiquement l'ordinateur à un poste de travail.

Pour obtenir des informations détaillées, consultez le *Manuel de référence du matériel* disponible sur le CD *Documentation Library*.

Identification des empreintes digitales

Tout en dispensant l'utilisateur de saisir des mots de passe, la technologie d'identification des empreintes digitales élaborée par HP renforce la sécurité du réseau, simplifie la procédure de connexion et réduit les coûts relatifs à la gestion des réseaux d'entreprise. Son coût abordable ne la réserve désormais plus aux seuls organismes de pointe disposant d'un système de sécurité très élaboré.



La prise en charge de la technologie d'identification des empreintes digitales varie en fonction des modèles.

Pour plus d'informations, consultez le site
http://www.compaq.com/products/quickspecs/10690_na/10690_na.html

Notification des pannes et récupération

Les fonctions de notification des pannes et de récupération allient des technologies matérielle et logicielle novatrices qui évitent la perte des données essentielles et réduit les temps d'inactivité imprévus.

Lorsqu'une panne survient, l'ordinateur affiche un message d'alerte local, contenant la description de la panne et la marche à suivre pour y remédier. Vous pouvez ensuite visualiser l'état actuel du système à l'aide de l'Agent de supervision HP. Si l'ordinateur est relié à un réseau supervisé par HP Insight Manager ou par d'autres produits de supervision des Partenaires Solutions de supervision Compaq, il envoie également une notification de panne à l'application de supervision du réseau.

Système de protection d'unité DPS

Le système de protection d'unité DPS (Drive Protection System) est un outil de diagnostic intégré aux disques durs installés sur certains ordinateurs HP. Le DPS est conçu pour aider au diagnostic des problèmes pouvant conduire à un remplacement du disque dur non pris en charge par la garantie.

Lors de la construction des ordinateurs HP, chaque disque dur installé est testé avec le système DPS, et un enregistrement permanent des informations clés est écrit sur le disque. À chaque test DPS, les résultats sont inscrits sur le disque dur. Votre mainteneur peut ensuite utiliser ces informations pour le diagnostic des pannes vous ayant conduit à exécuter le logiciel DPS. Reportez-vous au *Manuel de résolution des problèmes* pour la procédure d'utilisation du système DPS.

Surveillance de l'intégrité Ultra ATA

La fonction de Surveillance de l'intégrité Ultra ATA permet de contrôler l'intégrité des données lors de la transmission entre le disque dur Ultra ATA et la logique interne du système. Si l'ordinateur détecte un nombre anormal d'erreurs de transmission, il affiche un message d'alerte locale et vous indique la procédure à suivre pour remédier au problème.

Alimentation avec protection contre les surtensions

Un système intégré de protection contre les surtensions assure une plus grande fiabilité de l'ordinateur en cas de surtension imprévue. Cette alimentation peut supporter une surtension de 2000 volts sans temps d'arrêt du système, ni perte de données.

Détecteur thermique

Le capteur thermique est une fonction matérielle et logicielle qui contrôle la température interne de l'ordinateur. Cette fonction affiche un message d'alerte en cas de dépassement de la plage normale de températures, ce qui permet de prendre des mesures avant que les composants internes ne soient endommagés ou que des données ne soient perdues.

Index

A

- accès à l'ordinateur, contrôle 15
- ActiveUpdate 7
- Adresses Internet, voir Sites Web
- Adresses Web. Voir Sites Web
- alimentation, protection contre les surtensions 35
- Altiris eXpress 4
- Altiris eXpress HP/Compaq Client Manager 6
- Altiris eXpress PC Transplant Pro 5
- annulation d'un mot de passe 23
- AssetControl 15

B

- Bloc d'amorçage ROM FailSafe 9
- Bouton d'alimentation
 - double état 11
- Bouton d'alimentation
 - configuration 11
- bouton de mise sous tension double état 11

C

- Capteur thermique 35
- caractères de séparation selon les claviers 23
- caractères de séparation, tableau 23
- changement de mot de passe 21
- changement de système d'exploitation,
 - informations importantes 13
- clavier, caractères de séparation 23
- clé FailSafe
 - commande 30
 - précautions 30

- clé Smart Cover FailSafe, commander 30
- commande de la clé FailSafe 30
- configuration du bouton de mise sous tension 11
- configuration initiale 2
- configuration, réplication 11
- contrôle de l'accès à l'ordinateur 15

D

- définition
 - délais d'attente 12
 - détecteur Smart Cover 28
 - mot de passe de configuration 19, 21
 - mot de passe de démarrage 19
- délais d'attente, configuration 12
- Desktop Management Interface (DMI) 14
- détecteur Smart Cover
 - définition 28
 - niveaux de protection 27
- déverrouillage du verrou Smart Cover 29
- dispositif antivol 34
- disque amorçable, informations importantes 33
- disque, clonage 2
- disques durs, outil de diagnostic 35
- DMI (Desktop Management Interface) 14

E

- économies d'énergie, paramètres 12
- énergie, économies 12
- entrée
 - mot de passe de configuration 21
 - mot de passe de démarrage 20

F

fonctions de sécurité, tableau 16
formatage de disque, informations importantes 33

G

Gestion de l'alimentation 12

I

identification des empreintes digitales 34
installation à distance 3
Installation de système à distance, accès 3
installation initiale 2
intégrité des données 35

L

logiciel

- Altiris eXpress 4
- AssetControl 15
- Bloc d'amorçage ROM FailSafe 9
- Gestion de l'alimentation 12
- Installation de système à distance 3
- intégration 2
- Master Boot Record Security 31
- mise à jour de plusieurs ordinateurs 6
- Notification des pannes et récupération 34
- récupération 2
- Réécriture de la ROM à distance 8
- System Software Manager 6
- Système de protection d'unité DPS 35
- Utilitaires Computer Setup 11

logiciels préinstallés 2

M

mémoire morte non valide 9
mise à niveau de la ROM 8
mot de passe

- changement 21
- configuration 19, 21
- effacement 23
- mise sous tension 19, 20

- suppression 22

mot de passe de configuration

- changement 21
- définition 19
- entrée 21
- suppression 22

mot de passe de démarrage

- changement 21
- définition 19
- entrée 20
- suppression 22

N

notification de pannes 34

O

outil de diagnostic pour les disques durs 35
outils de clonage, logiciels 2
outils de déploiement, logiciels 2

P

partitionnement de disque, informations importantes 33
personnalisation des logiciels 2
Précautions

- protection de la ROM 8
- sécurité de verrouillage du capot 28

précautions

- clé FailSafe 30

Product Change Notification (PCN) 7
protection de la ROM, précaution 8
protection des disques durs 35

R

récupération du système 9
récupération, logiciels 2
Réécriture de la ROM à distance 8
ROM système non valide 9
ROM, mise à niveau 8
ROM, voyants du clavier, tableau 10

S

sécurité MBR, paramétrage 31

sécurité par mot de passe 18

sécurité, configuration 15

sécurité, MBR 31

Sites Web

www.compaq.com 8, 13

www.compaq.com/activeupdate 7

www.compaq.com/easydeploy 5, 6, 8, 11, 13

www.compaq.com/im/ssmwp.html 6, 8

www.compaq.com/pcn 7

www.compaq.com/products/quickspecs/10690_na/10690_na.html 34

www.compaq.com/solutions/pcsolutions 2

sites Web

www.compaq.com 30

Smart Cover, verrou 28

Supervision intelligente 14

suppression de mot de passe 22

Surveillance de l'intégrité Ultra ATA 35

System Software Manager (SSM) 6

Système de protection contre les surtensions 35

système, récupération 9

systèmes d'exploitation, informations importantes 13

T

technologies Wired for Management 14

température interne de l'ordinateur 35

température, à l'intérieur de l'ordinateur 35

U

unité, protection 35

URL (sites Web). Voir Sites Web

Utilitaires Computer Setup 11

V

Verrou Smart Cover

déverrouillage 29

verrouillage 29

verrouillage du capot, précautions de sécurité 28

verrouillage du verrou Smart Cover 29

voyants du clavier, ROM, tableau 10